공개 클라우드 기반 개인정보 및 악성 파일 탐지를 위한 자동화 보안 플랫폼 설계

정지용*, 이재윤*, 신동엽*, 정대영*
*네이버클라우드캠프, 이스트소프트
stopdragon00@gmail.com, jaeyoonleev@gmail.com,
ehdduq0307@gmail.com, hidae0az@gmail.com

Design of an Automated Security Platform for Detecting Personal Information and Malicious Files in Public Cloud Storage

Jung Ji yong*, Lee Jae Yoon*, Shin Dong Yeob*, Jeong Dae Young*
*Naver Cloud camp in Est soft

요 약

클라우드 오브젝트 스토리지는 대용량 비정형 데이터를 저장할 수 있는 유연한 인프라로 각광받고 있으나, 설정 오류로 인한 공개 저장소 발생과 그로 인한 개인정보 유출 문제가 심각해지고 있다. 본 연구에서는 이러한 위협에 대응하기 위해, 공개 출처 기반으로 정보를 수집하고 악성 코드와 개인정보를 자동으로 탐지하는 웹 기반 보안 시스템을 설계하였다. 제안된 시스템은 공개 클라우드 저장소의 버킷을 자동으로 탐색하고, 사전 정의된 확장자 기준으로 문서를 수집한 뒤, VirusTotal API를 통한 악성코드 진단, CLOVA OCR 기반 텍스트 추출, 그리고 대규모 언어모델을 이용한 개인정보 분석을 연계하여 탐지 과정을 자동화한다. 분석 결과는 웹 대시보드로 출력되며, 사용자는 웹 인터페이스를 통해 실시간 탐지 요청과 결과 확인, 보고서 다운로드까지 수행할 수 있다. 웹 기반으로 제공됨에 따라 비전문가도 손쉽게 시스템을 활용할 수 있어 접근성이 크게 향상된다. 본 시스템은 수작업 없이도 비정형 개인정보 탐지가 가능하다는 점에서 기존 방식 대비 실용성과 확장성을 갖추고 있으며, 공공 제보 시스템과의 연계 가능성도 제시한다.

Ⅰ. 서 론

클라우드 오브젝트 스토리지는 비용 효율성과 확장성을 기반으로 다양한 산업 분야에서 폭넓게 활용되고 있으며, 특히 비정형 데이터의 저장 및 공유 수단으로 빠르게 자리잡고 있다. 그러나 이러한 유연성은 동시에 보안 취약성을 수반한다. 설정 실수나 접근 제어의 부주의로 인해 민감한 문서가 외부에 무방비로 노출되는 사례가 지속적으로 발생하고 있으며, 이에 따라 개인정보 유출 사고도 함께 증가하는 추세다[1].

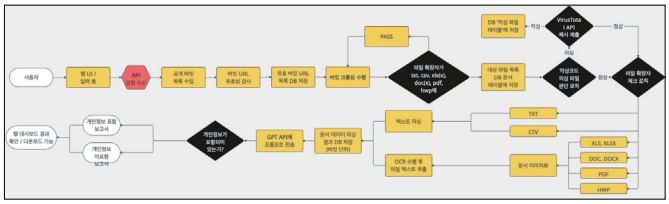
현재까지의 대응 방식은 주로 정규표현식 기반의 패턴 탐지나 명명된 개체 인식(NER) 기법에 의존해 왔다. 이러한 방식은 구조화된 텍스트나 형식이 명확한 데이터에는 유효하지만, 문맥적 의미나 비정형 표현이 포함된 문서에서는 탐지 정확도가 크게 떨어지는 한계가 있다[2].

본 연구에서는 이러한 문제를 해결하기 위해, 공개 출처 기반(Open Source Intelligence, OSINT) 데이터를 자동으로 수집하고, 문서 내 악성 코드 존재 여부와 개인정보 포함 여부를 종합적으로 분석하는 웹 기반 자동화 보안 시스템을 제안한다. 해당 시스템은 공개 클라우드 저장소의 버킷을 자동 탐색한 뒤, 유효 문서를 수집하고, 텍스트 추출 및 의미 분석을 통해 민감 정보를 식별하며, 결과를 보고서 형태로 자동 생성하여 사용자에게 웹 대시보드 형태로 제공한다.

Ⅱ. 본 론

2.1 시스템 구조

본 시스템은 공개 출처 기반 데이터를 자동으로 수집·분석하고 결과를 제공하는 웹 기반 자동화 보안 플랫폼으로, 사용자 요청부터 문서 처리 및 보고서 생성까지의 전 과정을 자동화된 파이프라인으로 구성하였다. 전체 처리 흐름은 <그림 1>에 제시하였다.



<그림 1> 시스템 플로우차트

2.2 공개 버킷 탐색 및 수집 절차

시스템은 사용자의 탐지 요청이 수신되면, 이를 기반으로 공개 클라우드 오브젝트 스토리지 내에서 유출 가능성이 있는 데이터를 자동으로 탐색한다. 이 과정에서는 공개 출처 기반 검색 플랫폼을 활용하며, 사용자가 입력한 키워드와 필터 조건을 기준으로 API 호출 또는 Selenium 기반 브라우저 자동화를 통해 공개 버킷 목록을 수집한다.

수집된 URL 목록은 중복 제거 및 형식 정규화를 거친 후, HTTP HEAD 및 GET 요청을 통해 실질적인 접근 가능 여부를 확인한다. 이 과정에서 응답 상태, 콘텐츠 타입, 파일 확장자 등 다양한 요소가 자동 검증되며, 정상 응답이 확인된 URL만이 유효 대상으로 분류된다.

유효한 버킷 URL과 해당 버킷 내 문서에 대한 메타데이터(파일 경로, 응답 상태, 확장자 등)는 외부 데이터베이스에 저장된다.

2.3 파일 수집 및 문서 저장

유효한 버킷 URL이 식별되면, 시스템은 해당 버킷에 직접 접근하여 문서 파일을 수집한다. 수집 대상은 사전에 정의된 확장자 기준에 따라 선별

되며, .txt, .csv, .xls(x), .doc(x), .pdf, .hwp, .jpg, .png등 개인정보를 포함할 가능성이 높은 문서 포맷만을 대상으로 한다.

각 문서 파일은 접근 경로, 파일명, 확장자, 수집 시각, 응답 코드 등으로 구성된 메타데이터와 함께 자동으로 정리되며, 문서 저장 전용 테이블에 구조화된 형태로 기록된다. 수집된 원본 파일은 무결성을 보장한 상태로 저장된다.

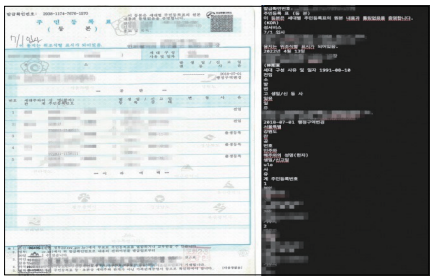
수집 프로세스는 단일 서버 내에서 병렬로 수행되도록 구성되어 있어 다수의 공개 버킷과 파일에 대해 빠르게 대응할 수 있으며, 수집된 파일은 전체 분석 파이프라인에서 가장 핵심적인 데이터 소스로 사용된다.

2.4 악성 여부 진단 및 문서 분석

수집된 문서 파일은 우선 VirusTotal API를 활용한 해시 기반 정적 분석을 통해 악성코드 여부를 판별한다[3].

이후 정상 파일에 대해서는 파일 형식에 따라 텍스트를 추출한다. .txt, .csv파일은 단순 파싱을 통해 처리되며, .pdf, .doc(x), .xls(x), .hwp, .jpg, .png등은 이미지로 변환 후 CLOVA OCR을 통해 텍스트를 추출한다. 이처럼 이미지 기반 문서까지도 자동 처리할 수 있도록 설계되어 있어 다양한 비정형 문서를 대응할 수 있다[4].

추출된 텍스트는 상용 LLM API에 전달되어 문맥 기반의 의미 분석이 수행된다. LLM은 일반적인 패턴 기반 탐지 방식과 달리, 문서 내 의미 구조와 문맥 흐름을 바탕으로 개인정보 포함 여부를 판단하며 정형, 비정형적 표현까지 인식할 수 있다. 분석 결과는 각 문서 단위로 기록되며, 이후 보고서 생성을 위한 핵심 자료로 활용된다.



<그림 2> 개인 정보 유출 문서 및 OCR 결과

2.5 보고서 자동 생성 및 결과 전달

문서별 개인정보 탐지 결과는 내부 기준에 따라 종합 정리되며, 각 문서에는 위험도 평가 점수가 부여된다. 이 평가 결과는 상용 LLM API에 전달될 특화된 프롬프트로 자동 변환되며, 프롬프트에는 문서 메타데이터, 탐지된 민감 정보의 유형, 판단 사유, 문맥 특징 등이 함께 포함된다.

LLM API는 이러한 입력을 바탕으로 문서 단위 보안 분석 결과를 서술형 형태로 응답하며, 시스템은 이 결과를 기반으로 웹 대시보드 형식의 보고서를 자동 생성한다. 보고서에는 위험 정보 요약, 주요 탐지 항목, 문서 내 민감 정보 위치 등의 정보가 포함되며, 공공기관 제보 시 요구되는 형식을 고려하여 구성되어 있다.

<그림 3> 자동 생성된 보안 분석 보고서 예시

본 시스템이 자동 생성한 보안 분석 보고서의 예시는 <그림 3>과 같다.

2.6 공개 출처 정보 탐지 결과

제안된 시스템의 성능을 검증하기 위해, 공개 출처 기반 검색 플랫폼을 활용하여 총 1,000개의 클라우드 오브젝트 스토리지 버킷을 대상으로 탐색 실험을 수행하였다. 이 중 280개는 접근이 가능한 저장소로 확인되었으며, 해당 버킷들로부터 총 4,500개의 문서가 수집되었다.

수집된 문서에 사전 정의된 확장자 필터를 적용한 결과, 3,200개 문서가 분석 대상에 포함되었고, 이들에 대해 VirusTotal API를 이용한 악성코드 검사를 수행하였다. 분석 결과, 126개 문서(3.94%)에서 악성코드가 탐지되어 이후 개인정보 분석 과정에서는 제외되었다.

나머지 3,074개 문서에 대해 CLOVA OCR을 통한 텍스트 추출과 LLM 기반 의미 분석을 진행한 결과, 672개 문서(22.51%)에서 비정형 개인정보가 포함된 것으로 탐지되었다.

본 실험을 통해 제안된 시스템이 다양한 문서 포맷에 대해 악성 여부를 효과적으로 판별하고, 정형뿐만 아니라 비정형 개인정보까지 높은 정확도로 식별할 수 있음을 확인하였다. 특히, LLM 기반 문맥 분석을 통해 기존 탐지 방식으로는 놓칠 수 있는 민감 정보까지 포착할 수 있었으며, 전 과정을 웹 기반에서 자동으로 처리함으로써 실시간 대응력과 사용자 접근성 측면에서도 강점을 입증하였다.

Ⅲ. 결론

본 연구는 클라우드 오브젝트 스토리지의 설정 오류로 인해 발생할 수 있는 개인정보 유출 위협에 대응하기 위해, 공개 출처 탐색, 문서 수집, 악성코드 진단, 개인정보 분석, 보고서 자동 생성을 통합한 웹 기반 보안 시스템을 설계하고 구현하였다.

제안된 시스템은 공개 클라우드 상의 유출 가능성이 있는 데이터를 자동으로 탐색하고, 문서 유형에 따라 적절한 분석 절차를 적용함으로써 정형 및 비정형 개인정보를 효과적으로 탐지할 수 있다. 특히 LLM 기반 문맥 분석과 CLOVA OCR 기반 비정형 문서 처리 기능을 연계함으로써, 기존의 패턴 중심 탐지 기법이 가진 한계를 보완하고, 다양한 파일 포맷에 대한 유연한 대응이 가능함을 확인하였다.

해당 플랫폼은 현재 웹사이트 형태로 운영 중이며, 사용자는 탐지 요청부터 결과 확인, 보고서 다운로드까지 모든 과정을 웹 대시보드를 통해 실시간으로 수행할 수 있다. 이를 통해 비전문가도 손쉽게 민감 정보 유출 여부를 점검하고 대응할 수 있으며, 실용성과 접근성 측면에서도 높은 활용 가능성을 가진다.

향후에는 고위험 문서에 대한 자동 경고 기능, KISA 제보 자동화, 다국어 문서 지원, 도메인 특화 LLM 적용 등을 통해 시스템의 분석 정확도와 보안 대응 능력을 지속적으로 고도화할 계획이다.

참 고 문 헌

[1] Amazon Web Services, "Amazon S3 Security Best Practices," AWS Whitepaper, 2020.

[2] V. Kuzina, E. Vušak, and A. Jović, "Methods for Automatic Sensitive Data Detection in Large Datasets: a Review," 2021.

[3] VirusTotal, "VirusTotal Official API Documentation," 2022.

[4] Naver CLOVA, "CLOVA OCR API Guide," Naver Developer Center, 2022.